EXHIBIT A

Supreme Court of Pennsylvania

Court of Common Pleas
Civil Cover Sheet

Lackawanna County

For Prothonotary Use Only:	
Docket No:	

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

SECTION A

Commencement of Action:
- [x] Complaint
- [ ] Writ of Summons
- [ ] Petition
- [ ] Transfer from Another Jurisdiction
- [ ] Declaration of Taking

Lead Plaintiff's Name:	Lead Defendant's Name:
Dennis Ross	Community Health Systems, Inc.
Are money damages requested? [x] **Yes** [ ] **No**	Dollar Amount Requested: (check one) [ ] within arbitration limits [x] outside arbitration limits
Is this a *Class Action Suit?* [x] **Yes** [ ] **No**	**Is this an *MDJ Appeal?*** [ ] **Yes** [x] **No**

Name of Plaintiff/Appellant's Attorney: Richard Shenkan

[ ] **Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)**

SECTION B

Nature of the Case: Place an "X" to the left of the **ONE** case category that most accurately describes your ***PRIMARY CASE.*** If you are making more than one type of claim, check the one that you consider most important.

TORT (*do not include Mass Tort*)
- [ ] Intentional
- [ ] Malicious Prosecution
- [ ] Motor Vehicle
- [ ] Nuisance
- [ ] Premises Liability
- [ ] Product Liability (*does not include mass tort*)
- [ ] Slander/Libel/ Defamation
- [x] Other: Negligence - Data Breach

MASS TORT
- [ ] Asbestos
- [ ] Tobacco
- [ ] Toxic Tort - DES
- [ ] Toxic Tort - Implant
- [ ] Toxic Waste
- [ ] Other:

PROFESSIONAL LIABLITY
- [ ] Dental
- [ ] Legal
- [ ] Medical
- [ ] Other Professional:

CONTRACT (*do not include Judgments*)
- [ ] Buyer Plaintiff
- [ ] Debt Collection: Credit Card
- [ ] Debt Collection: Other
- [ ] Employment Dispute: Discrimination
- [ ] Employment Dispute: Other
- [ ] Other:

REAL PROPERTY
- [ ] Ejectment
- [ ] Eminent Domain/Condemnation
- [ ] Ground Rent
- [ ] Landlord/Tenant Dispute
- [ ] Mortgage Foreclosure: Residential
- [ ] Mortgage Foreclosure: Commercial
- [ ] Partition
- [ ] Quiet Title
- [ ] Other:

CIVIL APPEALS
Administrative Agencies
- [ ] Board of Assessment
- [ ] Board of Elections
- [ ] Dept. of Transportation
- [ ] Statutory Appeal: Other
- [ ] Zoning Board
- [ ] Other:

MISCELLANEOUS
- [ ] Common Law/Statutory Arbitration
- [ ] Declaratory Judgment
- [ ] Mandamus
- [ ] Non-Domestic Relations Restraining Order
- [ ] Quo Warranto
- [ ] Replevin
- [ ] Other:

Updated 1/1/2011

IN THE COURT OF COMMON PLEAS
OF LACKAWANNA COUNTY

DENNIS ROSS and ANGELA SCHUH, on behalf of themselves and all others similarly situated,	)	Case No.
Plaintiff,	)	**JURY TRIAL DEMANDED**
v.	)	
COMMUNITY HEALTH SYSTEMS, INC., CHSPSC, LLC, WILKES-BARRE HOSPITAL COMPANY, LLC, d/b/a COMMONWEALTH HEALTH, MOSES TAYLOR HOSPITAL, REGIONAL HOSPITAL OF SCRANTON, SCRANTON HOSPITAL COMPANY, LLC, and WILKES-BARRE GENERAL HOSPITAL,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Dennis Ross and Angela Schuh ("Plaintiffs") file this Class Action Complaint on behalf of themselves, and all others similarly situated, against Defendants Community Health Systems, Inc. ("CHS"), CHSPSC, LLC ("CHSPSC"), Wilkes-Barre Hospital Company ("WBHC"), doing business as Commonwealth Health, Moses Taylor Hospital, Regional Hospital of Scranton, Scranton Hospital Company, LLC, and Wilkes-Barre General Hospital (collectively "Defendants"), and allege as follows:

NATURE OF THE ACTION

1. Healthcare providers that handle sensitive, personally identifying information ("PII") or protected health information ("PHI") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a data and privacy breach manifests in a number of ways, including identity theft and financial fraud, and the exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

3. Defendants are healthcare providers, and as such, Defendants knowingly obtain sensitive patient PII and PHI and have a resulting duty to securely maintain such information in confidence.

4. On February 13, 2023, Defendant CHSPSC disclosed to the Securities and Exchange Commission that their secure file transfer platform was accessed by unauthorized parties, compromising the patient PII and PHI stored therein (the "Data Breach").[1]

5. The notorious Clop ransomware gang took responsibility for the Data Breach.[2]

6. Based on the public statements of Defendants to date, a wide variety of PII and PHI was implicated in the Data Breach, including but not limited to an individuals' full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and Social Security number.[3]

---

[1] Dissent, *Community Health Systems Estimates 1 million patients impacted by vendor's GoAnywhere breach*, DataBreaches.net (Feb. 13, 2023), https://www.databreaches.net/community-health-systems-estimates-1-million-patients-impacted-by-vendors-goanywhere-breach/.

[2] Sergiu Gatlan, *Healthcare giant CHS reports first data breach in GoAnywhere hack*, BleepingComputer (Feb. 14, 2023), https://www.bleepingcomputer.com/news/security/healthcare-giant-chs-reports-first-data-breach-in-goanywhere-hacks/.

[3] *Notice of Data Breach*, *supra.* note 1.

7. As a direct and proximate result of Defendants' failure to implement and follow basic security procedures, Plaintiffs' and Class Members' PII and PHI is now in the hands of cybercriminals.

8. Plaintiffs and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiffs and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

9. Plaintiffs, on behalf of themselves as individuals and all others similarly situated, allege claims for negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, and declaratory judgment. Plaintiffs seek damages and injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII and PHI in Defendants' custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

10. Plaintiff Dennis Ross is an adult, who at all relevant times, is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff Ross was a patient at one or more of the Defendant hospitals in Pennsylvania. Plaintiff Ross received a Data Breach notice from Defendant CHSPSC informing him that his PII and PHI that he entrusted to Defendants was compromised in the Data Breach.

11. Plaintiff Angela Schuh is an adult, who at all relevant times, is a resident and citizen of the Commonwealth of Pennsylvania. Plaintiff Schuh was a patient at one or more of the Defendant hospitals in Pennsylvania. Plaintiff Schuh received a Data Breach notice from Defendant CHSPSC informing her that her PII and PHI that she entrusted to Defendants was compromised in the Data Breach.

12. As a result of the Data Breach, Plaintiffs will continue to be at a heightened and certainly impending risk for fraud and identity theft, and their attendant damages for years to come.

13. Defendant CHS is a Delaware corporation with a principal place of business located at 4000 Meridian Blvd., Franklin, Tennessee 37067. Defendant CHS is the ultimate parent company of Defendant CHSPSC.

14. Defendant CHSPSC is a Delaware limited liability company with a principal place of business located at 4000 Meridian Blvd., Franklin, Tennessee 37067. Defendant CHSPSC is a single member limited liability company, and upon information and belief, that sole member is Defendant CHS. Defendant CHSPSC is a citizen of each state in which one of its members is a citizen. As such, Defendant CHSPSC is a citizen of the State of Pennsylvania.

15. Defendant Wilkes-Barre Hospital Company is a Delaware limited liability company, and a majority owned subsidiary of CHS, with a principal place of business located at 4000 Meridian Blvd., Franklin, Tennessee 37067.

16. Defendant Commonwealth Health is a fictitious name owned by Defendant Wilkes-Barre Hospital Company, with a principal address of 575 North River Street, Wilkes Barre, PA 18764.

17. Scranton Hospital Company is a Delaware limited liability company, and a majority owned subsidiary of CHS, with a principal place of business located at 4000 Meridian Blvd., Franklin, Tennessee 37067.

18. Defendant Moses Taylor Hospital is a fictitious name owned by Scranton Hospital Company, with a principal address of 700 Quincy Ave, Scranton, PA 18510.

19. Defendant Regional Hospital of Scranton is a fictitious name owned by Scranton Hospital Company, with a principal address of 746 Jefferson Ave., Scranton, PA 18510.

20. Defendant Wilkes-Barre General Hospital is a fictitious name owned by Defendant Wilkes-Barre Hospital Company, with a principal address of 575 North River Street, Wilkes Barre, PA 18764.

JURISDICTION AND VENUE

21. This Court subject matter jurisdiction over this action pursuant to 42 Pa.C.S. 931.

22. This Court has personal jurisdiction over Defendants pursuant to 42 Pa.C.S. 5301(a)(2).

23. Venue is proper in Lackawanna County pursuant to Pa.R.Civ.P. 2179 because, *inter alia*, each Defendant avails itself to Lackawanna County by conducting substantial and significant business there. In addition, a large number of class members affected by this Data Breach reside in Lackawanna County.

FACTUAL BACKGROUND

A. Defendants and the Services They Provide.

24. Defendants CHS, who is the ultimate parent company of all Defendants, touts itself as one of the nation's largest providers of healthcare services, operating hospitals and other facilities across fifteen states.

25. Upon information and belief, while Defendants administer healthcare services, Defendants receive, maintain, and handle PII and PHI from their patients, which includes, inter-alia, full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and Social Security number.

26. Plaintiffs and Class Members directly or indirectly entrusted Defendants with their sensitive and confidential PII and PHI and therefore reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

27. As a custodian of Plaintiffs' and Class Members' PII and PHI, Defendants assumed equitable and legal duties to safeguard and keep confidential Plaintiffs' and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

28. Each Defendant has a privacy policy and/or practice that states that it is committed to protecting the personal and/or medical information it collects, uses, and/or discloses. Despite these policies, Defendants nevertheless failed to secure the PII and PHI of the individuals that provided them with sensitive information, resulting in the Data Breach and compromise of Plaintiffs' and Class Members' PII and PHI.[4]

29. Defendants' data security obligations have increased in importance given the substantial increase in cyber-attacks and/or data breaches preceding the date it disclosed the Data Breach.

B. Defendants Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims.

30. Defendants were well aware that the PHI and PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

31. Defendants also knew that a breach of their systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

32. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

[4] *Notice of Data Breach, supra.* note 1.

33. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[5] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

34. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[6]

35. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[7]

36. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[8] This is in part because now more than ever, healthcare

---

[5] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[6] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[7] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 25, 2023).

[8] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Apr. 25, 2023).

companies "are using electronic records and tapping digital services" "creating more opportunities for cybercriminals."

37. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[9]

38. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals—"[t]hat equates to more than 1.2x the population of the United States."[10]

39. Further, the rate of healthcare data breaches has been on the rise in recent years. "In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[11]

40. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[12]

---

[9] *Id.*

[10] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Apr. 24, 2023).

[11] *Id.*

[12] *2022 Breach Barometer*, PROTENUS, https://www.protenus.com/breach-barometer-report (last visited Apr. 25, 2023).

41. According to Fortified Health Security's mid-year report released in July 2022, the healthcare sector suffered about 337 breaches in the first half of 2022 alone. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[13]

42. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

43. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[14] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[15]

44. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.

---

[13] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

[14] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[15] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Apr. 25, 2023).

> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[16]

45. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[17]

46. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

---

[16] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[17] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 25, 2023).

47. Based on the value of its patients' PII and PHI to cybercriminals, Defendants certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Defendants Show a Reckless Disregard for Data Security.

48. As members of one of the largest healthcare providers in the United States, Defendants have an obligation to securely maintain the PII and PHI that it is entrusted and keep it safe from harm. Defendants know that the PII and PHI they collect and maintain are prime targets for cybercriminals. Yet, Defendants have major security problems that pose a threat to their patients' sensitive information.

49. The current Data Breach is not the first time that Defendants have failed to protect their patients PII and PHI from actors with nefarious intentions. In 2014, CHS suffered a data breach during which hackers installed malware on Defendants' computer systems, compromising the PHI of 6.1 million individuals.[18] The information compromised during the 2014 data breach included names, phone numbers, addresses, dates of birth, sex, ethnicity, Social Security numbers, and emergency contact information.[19]

50. As a result of the 2014 data breach, CHS was investigated by Health and Human Services' Office of Civil Rights ("OCR"). An audit completed by OCR revealed that CHS had failed to implement security protections as required by the Health Insurance and Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1302d, *et seq.*[20] Indeed, according to the agency, "OCR's investigation found longstanding, systemic noncompliance with the HIPAA Security Rule

---

[18] *Community Health Systems Pay $5 Million to Settle Multi-State Breach Investigation*, HIPAA Journal (Oct. 9, 2020), https://www.hipaajournal.com/community-health-systems-pays-5-million-to-settle-multi-state-breach-investigation/.

[19] *Id.*

[20] Hannah Ruhoff, *Mississippi Health-Care System Reports Data Breach*, Government Technology (Mar. 9, 2023), https://www.govtech.com/security/mississippi-health-care-system-reports-data-breach.

including failure to conduct a risk analysis, and failures to implement information system activity review, security incident procedures, and access controls."[21]

51. To resolve CHS's potential violations of HIPAA, in 2020 CHS agreed to pay $2.3 million dollars to OCR and implement and maintain new cybersecurity measures to safeguard PHI.[22]

52. Despite Defendants' "new" cybersecurity plan, CHS nevertheless suffered a second data breach less than three years later, again compromising patients' sensitive information.

D. Defendants Breached Their Duty to Protect PII and PHI.

53. All Defendants engaged Fortra LLC's ("Fortra") to provide them with a secure file transfer software—GoAnywhere MFT. "The GoAnywhere MFT is a web-based and managed file transfer tool designed to help organizations transfer files securely with partners and keep audit logs of who accessed the shared files."[23]

54. However, the GoAnywhere MFT software contained a major security vulnerability that could be exploited by criminal actors who wished to steal sensitive data contained on the file transfer platform.

55. In mid-February 2023, CHS announced that they had been impacted by a security incident involving the GoAnywhere MFT software.[24]

---

[21] Kat Jercich, *OCR levies $2.3M fine over massive breach affecting PHI of 6M people*, Healthcare News (Spt. 24, 2020), https://www.healthcareitnews.com/news/ocr-levies-23m-fine-over-massive-breach-affecting-phi-6m-people.

[22] *Id.*

[23] Sergiu Gatlan, *Exploit released for actively exploited GoAnywhere MFT zero-day*, BleepingComputer (Feb. 6, 2023), https://www.bleepingcomputer.com/news/security/exploit-released-for-actively-exploited-goanywhere-mft-zero-day/.

[24] *Community Health Systems to Notify Up to 1 Million Individuals About GoAnywhere Data Breach*, HIPAA Journal (Mar. 10, 2023), https://www.hipaajournal.com/community-health-systems-goanywhere-data-breach/.

56. According to CHSPSC, between January 28 and January 30, 2023, Fortra discovered that unauthorized parties gained access to the GoAnywhere MFT software, compromising sets of files throughout the file transfer platform.[25]

57. On or about February 2, 2023, Defendants were then notified of the Data Breach and initiated their own investigation to determine the extent to which patient information was impacted.[26]

58. CHSPSC'S investigation confirmed that wide swaths of sensitive information were exposed during the Data Breach including an individual's full name, address, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as date of birth and social security number.[27]

59. The notorious Clop ransomware gang has since claimed responsibility for the Data Breach, informing website BleepingComputer that Clop breached and stole data from over 130 organizations who utilized the GoAnywhere MFT software.[28] Clop was able to breach GoAnywhere MFT software by successfully exploiting a zero-day vulnerability which allowed the hackers to create unauthorized user accounts and leverage those user accounts to download files contained in the file share platform.[29]

60. On or about March 16, 2023, Defendants reported the Data Breach to OCR, indicated that approximately 962,000 individuals were impacted by the Data Breach.[30]

---

[25] *Notice of Data Breach*, *supra* note 1.
[26] *Id.*
[27] *Notice of Data Breach*, *supra* note 1.
[28] Gatlan, *supra* note 3.
[29] Ravie Lakshmanan, *Fortra Shed light on GoAnywhere MF Zero-Day Exploit used in Ransomware Attacks*, The Hacker News (Apr. 20, 2023), https://thehackernews.com/2023/04/fortra-sheds-light-on-goanywhere-mft.html.
[30] *Breach Portal*, U.S. Dep't of Health & Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, (last visited Apr. 25, 2023).

61. Despite discovering the Data Breach in early February, impacted patients did not begin to be informed by any Defendant for over a month. Indeed, Plaintiffs did not receive a data breach notice informing them that their PII and PHI had been compromised during the Data Breach until on or about March 24, 2023.

62. Upon information and belief, Class Members received similar Data Breaches notices on or around March 24, 2023, informing them that their PII and/or PHI was exposed during the Data Breach.

63. On or about April 17, 2023, Defendant CHSPSC issued a supplemental notice on the website of the Office of the Maine Attorney General, indicating the Data Breach was larger than initially reported and actually impacted approximately 1,173,000 individuals.[31]

64. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic data security procedures in order to protect individuals' PII and PHI. Defendants could have prevented the Data Breach, or substantially mitigated its severity, if they properly screened their vendors or contractors, such as Fortra, for cybersecurity standards as well as conducting cybersecurity audits of their contractors and vendors.

E. Defendants Are Obligated Under HIPAA to Safeguard Personal Information.

65. Defendants are "covered entities" under HIPAA (45 CFR § 160.103) and are required by HIPAA to safeguard patient PHI.

66. HIPAA sets minimum federal standards for privacy and security of PHI.

---

[31] *Data Breach Notifications*, Office of the Maine Attorney General (Apr. 17, 2023), https://apps.web.maine.gov/online/aeviewer/ME/40/810b151b-febe-43ef-9b77-b4c8ea0d9f4d.shtml.

67. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

68. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

69. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

70. HIPAA requires Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq.*

71. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[32]

72. While HIPAA permits healthcare providers and their business associates to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers and their business associates to disclose PHI to cybercriminals nor did Plaintiffs or the Class Members consent to the disclosure of their PHI to cybercriminals.

73. As such, Defendants are required under HIPAA to maintain the strictest confidentiality of Plaintiffs' and Class Members' PHI that it acquires, receives, and collects, and Defendants are further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

74. Given the application of HIPAA to Defendants, and that Plaintiffs and Class Members directly or indirectly entrusted their PHI to Defendants in order to receive healthcare services from Defendants, Plaintiffs and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

F. FTC Guidelines Prohibit Defendants from Engaging in Unfair or Deceptive Acts or Practices.

75. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

---

[32] *Breach Notification Rule*, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

76. The FTC Act does not define unfair or deceptive acts or practices, but the FTC can declare acts and practices to be unfair or deceptive, so long as "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. §45(n).

77. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[33]

78. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[34]

79. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[35]

80. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

---

[33] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[34] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[35] *Id.*

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act.[36] Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

81. Defendants were at all times fully aware of their obligations to protect the PII and PHI of patients because of their position as healthcare providers who stored patient PII and PHI. Defendants were also aware of the significant repercussions that would result from their failure to do so.

82. Despite their obligations, Defendants failed to properly implement reasonable and appropriate data security practices, and Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

G. Plaintiffs and Class Members Have Suffered Damages.

83. As a result of Defendants' failure to implement and follow reasonable and appropriate security procedures and failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI, Plaintiffs' and Class Members' PII/PHI has been and is now in the hands of unauthorized individuals, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals and entities. Plaintiffs and other Class Members now face an increased risk of identity theft, and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to the Data Breach.

84. Plaintiffs and other Class Members have had their most sensitive PII/PHI disseminated to the public at large and have experienced and will continue to experience emotional

[36] https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement

pain and mental anguish and embarrassment.

85. Plaintiffs and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

86. PII/PHI is a valuable property right.[37] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[9] American companies are estimated to have spent over $19 billion acquiring personal data of consumers in 2018.[10] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

87. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims, including Plaintiffs and Class Members.

88. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire

---

[37] *See* Marc van Lieshout, *The Value of Personal Data* at p. 4, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 10, 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]") (last visited Apr. 25, 2023).

company data breaches from $900 to $4,500.[13]

89. PHI is particularly valuable. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[38] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[39]

90. Recognizing the high value that consumers place on their PII/PHI, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII/PHI.[40] This business has created a new market for the sale and purchase of this valuable data.[41]

91. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[42]

---

[38] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC Magazine (July 16, 2013), https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.

[39] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[40] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010), https://www.nytimes.com/2010/07/18/business/18unboxed.html.

[41] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, WSJ (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576 160764037920274.

[42] Janice Y. Tsai, *et al.*, *The Effect of Online Privacy Information on Purchasing Behavior, An*

92. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

93. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and prepared for a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[43]

94. Plaintiffs and Class Members, as a whole, as a result of the Data Breach, must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

95. Once PII/PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendants' conduct. Further, the value of Plaintiffs' and Class Members' PII/PHI has been diminished by its exposure in the Data Breach.

Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1 (last visited March 1, 2023).

[43] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

96. As a result of Defendants' failures, Plaintiffs and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PII/PHI.

97. Plaintiffs and the Class suffered actual injury from having PII/PHI compromised as a result of Defendants' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII/PHI, a form of property that Defendants obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

98. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiffs and members of the Class these significant injuries and harm.

CLASS ALLEGATIONS

99. Plaintiffs bring this case individually and, pursuant to the Pennsylvania Rules of Civil Procedure, on behalf of the following class:

All individuals:

(1) whose PII and/or PHI was collected or maintained in Pennsylvania by CHS, CHSPSC, WBHC, Commonwealth Health, Moses Taylor Hospital, Regional Hospital of Scranton, Scranton Hospital Company, and/or Wilkes-Barre General Hospital, and,

(2) whose PII and/or PHI was compromised in the Data Breach that occurred between on or about January 28 and January 30, 2023 or to whom any Defendant sent a letter, to a mailing address in Pennsylvania, to inform of a data breach concerning his/her/their respective PII and/or PHI. (the "Class").

100. Excluded from the Class are Defendants, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendants have a controlling interest, the judicial officer(s) to whom this action is assigned, and the members of their immediate families, and the legal representative, heirs, successors, or assigns of any such excluded party.

101. This proposed class definition is based on the information available to Plaintiffs at this time. Plaintiffs expressly reserve their right to modify the class definition as necessary to account for any newly learned or changed facts as this case progresses.

102. Plaintiffs expressly reserve their right to as necessary, conduct a review of the Defendants records to ascertain the class members.

103. **Numerosity:** Plaintiffs, upon information and belief, allege there are hundreds to thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendants' records, including but not limited to the files implicated in the Data Breach.

104. **Commonality:** This action involves questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendants have a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Defendants were negligent in collecting and storing Plaintiffs' and Class Members' PII and PHI, and breached their duties thereby;

c. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

d. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

105. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Defendants were the custodian of Plaintiffs' and Class Members' PII and PHI, when their PII and PHI was obtained by an unauthorized third party.

106. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the members of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiffs have retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical as explained above.

107. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than separate individual cases for each Class Member, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

108. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiffs and each member of the Class. If Defendants breached their duty to Plaintiffs and Class Members, then Plaintiffs and each Class Member suffered damages by that conduct.

109. **Injunctive Relief:** Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under the Pennsylvania Declaratory Judgments Act, 42 Pa.C.S. §7531., *et seq*.

110. **Ascertainability:** Members of the Class are ascertainable. Class Membership is defined using objective criteria, and Class Members may be readily identified through Defendants' books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

111. Plaintiffs restate and reallege all of the paragraphs above as if fully set forth herein.

112. Defendants owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and/or misused by unauthorized persons.

113. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

114. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By receiving, maintaining, and handling PII and PHI that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

115. Defendants' duty also arose from Defendants' position as healthcare providers. Defendants held, and hold, themselves out as trusted providers of healthcare services, and thereby assumed a duty to reasonably protect the information they obtain from their patients. Indeed, Defendants, who receive, maintain, collect, and handle PII and PHI from their patients, were in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

116. Defendants breached the duties owed to Plaintiffs and Class Members and thus were negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiffs at this time, on information and belief, Defendants breached their duties through some combination of the following errors and omissions that allowed the Data Breach to occur: (a) mismanaging their computer systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their data security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies and practices; (h) failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII or PHI; and (i) failing to adequately vet third-party vendors before hiring them in connection with data security.

117. As a direct and proximate result of Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, their PII and PHI was compromised.

118. At the time of the Data Breach, the computer systems containing Plaintiffs' and Class Members' data were under the exclusive management and control of the Defendants, and the Data Breach would not have occurred in the ordinary course of events if ordinary care had been used to protect the data. Thus, pursuant to *res ipsa loquitur*, there was a breach of duty by the Defendants, and negligence by the Defendants can be inferred.

119. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

120. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

121. Plaintiffs restate and reallege all of the paragraphs above as if fully set forth herein.

122. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendants' duty.

123. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving the PII and PHI they were entrusted from their patients.

124. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

125. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

126. Defendants are entities covered under the HIPAA, which sets minimum federal standards for privacy and security of PHI.

127. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendants had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiffs' and the Class Members' electronic PHI.

128. Specifically, HIPAA required Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

129. Defendants violated HIPAA by actively disclosing Plaintiffs' and the Class Members' electronic PHI; and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI.

130. Plaintiffs and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients of Defendants.

131. Defendants' violation of HIPAA constitutes negligence *per se*.

132. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

133. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches

so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

134. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class)

135. Plaintiffs incorporates all preceding paragraphs as if fully set forth herein.

136. As a condition of obtaining services from Defendants, Plaintiffs and Class Members gave Defendants their PII/PHI in confidence, believing that they would protect that information. Plaintiffs and Class Members would not have provided Defendants will this information had they known it would not be adequately protected.

137. Defendants' acceptance and storage of Plaintiffs' and Class Members' PII/PHI created a fiduciary relationship between Defendants and Plaintiffs and Class Members. In light of this relationship Defendants must act primarily for the benefit of their and their affiliates patients, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

138. Defendants has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PII/PHI,

failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard the PII/PHI they collected.

139. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; (vii) loss of value of their PII/PHI, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

140. Plaintiffs incorporates all preceding paragraphs as if fully set forth herein.

141. In connection with receiving health care services, Plaintiffs and Class Members entered into implied contracts with Defendants.

142. Pursuant to these implied contracts, Plaintiffs and Class Members benefitted Defendants, directly or through an affiliate, by paying monies to Defendants, and provided Defendants with their PII/PHI. In exchange, Defendants agreed to, among other things, and Plaintiffs and Class Members understood that Defendants would: (1) provide products, services, or employment, to Plaintiffs and Class Members; (2) take reasonable measures to protect the

security and confidentiality of Plaintiffs' and Class Members' PII/PHI; (3) protect Plaintiffs' and Class Members' PII/PHI in compliance with federal and state laws and regulations and industry standards; and (4) ensure third parties they contract with and provide PII/PHI to implement and maintain reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' PII/PHI.

143. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Defendants, on the other hand. Indeed, as set forth *supra*, Defendants recognized the importance of data security and the privacy of their and their affiliates' patients' and employees' PII/PHI. Had Plaintiffs and Class Members known that Defendants would not adequately protect their PII/PHI, they would not have paid for products or services from Defendants.

144. Plaintiffs and Class Members performed their obligations under the implied contract when they provided Defendants with their PII/PHI and paid for products and services from Defendants or their affiliates, expecting that their PII/PHI would be protected.

145. Defendants breached their obligations under their implied contracts with Plaintiffs and Class Members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

146. Defendants' breach of their obligations of the implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach and the resulting injuries to Plaintiffs and Class Members.

147. Plaintiffs and all other Class Members were damaged by Defendants' breach of implied contracts because: (i) they paid monies (directly or through their insurers or Defendants

affiliates) in exchange for data security protection they did not receive; (ii) they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE CLASS)

148. Plaintiffs restate and reallege all of the paragraphs above as if fully set forth herein.

149. Under the Pennsylvania Declaratory Judgment Act, 42 Pa.C.S. §7531, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

150. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII and PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII and PHI. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and PHI and remains at imminent risk that further compromises of their PII and/or PHI will occur in the future.

151. Pursuant to its authority under the Pennsylvania Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure patient PII and PHI obtained from their patients and to timely notify such patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA.

b. Defendants breached and continue to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

152. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

153. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach of Plaintiffs' data held by Defendants occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

154. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

155. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another breach of data held by

Defendants, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and consumers whose confidential information would be further compromised.

SIXTH CAUSE OF ACTION
UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
(ON BEHALF OF PLAINTIFF AND THE CLASS)

156. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

157. The Unfair Trade Practices and Consumer Protection Law, 73 P.S. §201-1, *et seq.* ("UTPCPL") declares that "Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce as defined by subclauses (i) through (xxi) of clause (4) of section 21 of this act and regulations promulgated under section 3.12 of this act are hereby declared unlawful." 73 P.S. §201.3(a).

158. By concealing the Data Breach and failing to disclose the Data Breach to their customers (including Plaintiffs and Class Members) for over six weeks, and by failing to disclose to their customers (including Plaintiffs and Class Members) that they had not implemented and/or maintained reasonable security and practices to protect their PII/PHI, Defendants engaged in the following unfair methods of competition and unfair and deceptive acts and practices in violation of the UTPCPL:

a. Representing that goods or services have characteristics or benefits that they do not. (73 P.S. §201-2(v);

b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 §P.S. 201-2(vii);

c. Advertising goods or services with intent not to sell them as advertised (73 §P.S. 201-2(ix);

d. Failing to comply with the terms of any written guarantee or warranty given to the buyer at, prior to or after a contract for the purchase of goods or services is made (73 P.S. §201-2(xiv);

e. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. §201-2(xxi).

159. Defendants owed Plaintiffs and Class Members, among others, a duty to disclose these facts because they were known and/or accessible exclusively to Defendants who had exclusive and superior knowledge of the facts; because the facts would be material to reasonable consumers; because Defendants actively concealed them; and/or because Defendants intended for consumers to rely on the omissions in question.

160. Defendants' aforesaid conduct created a likelihood of confusion and/or misunderstanding for reasonable consumers, including Plaintiffs and Class Members, because

a. its customers, including Plaintiffs and Class Members, were not told of the inadequacy of Defendant's protection of their PII/PHI, which created a likelihood of confusion and misunderstanding as to the services provided by Defendant, and such knowledge would have been a material and substantial factor in their decision of whether to obtain or continue to obtain services from the Defendant; and/or

b. it did not inform its customers, including Plaintiff and Class Members, of the Data Breach for over six weeks, thus they were not able to take immediate steps to protect their PII/PHI.

161. Plaintiffs and Class Members justifiably relied on the aforesaid material representations and omissions of the Defendants.

162. Defendants' aforesaid acts and omissions were reckless, intentional, willful, and or wanton. Defendants were aware that they had inadequate security to protect Plaintiffs and Class Members' PII/PHI and was aware of the Data Breach, yet they made the decision not to notify Plaintiffs and Class Members of this material information.

163. As a result of Defendants' use of unfair methods of competition and unfair and deceptive acts and practices in violation of the UTPCPL, Plaintiffs and Class Members have suffered damages.

164. Plaintiffs and Class Members are entitled to an award of actual damages or $100, whichever is greater, costs, reasonable attorney's fees, and any additional relief this Court deems necessary or proper, including treble damages, punitive damages, and equitable relief. 73 P.S. §201-9.2 (a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under the Pennsylvania Rules of Civil Procedure and naming Plaintiffs as representative of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For treble damages and punitive damages;

e. For an order of restitution and all other forms of equitable monetary relief;

f. Declaratory and injunctive relief as described herein;

g. Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

h. Awarding pre- and post-judgment interest on any amounts awarded; and

i. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Respectfully submitted,
SHENKAN INJURY LAWYERS, LLC.
/s/ Richard Shenkan

P.O. Box 7255
New Castle, PA 16107
Telephone: (800) 601-0808
Facsimile: (888) 769-1774
rshenkan@shenkanlaw.com
Attorney for Plaintiffs

VERIFICATION

I verify that the averments of fact made in this pleading are true and correct and based upon my personal knowledge, information and belief. I understand that averments of fact are made subject to the penalties of 18 PA C.S. Section 4904 relating to unsworn falsification to authorities.

Dennis Ross

VERIFICATION

I verify that the averments of fact made in the pleading are true and correct and based upon my personal knowledge, information and belief. I understand that averments of fact are made subject to the penalties of 18 PA C.S. Section 4904 relating to unsworn falsification to authorities.

Angela Shuh